

# A General Construction of Binary Sequences with Optimal Autocorrelation

Tongjiang Yan <sup>a,b</sup> Zhixiong Chen <sup>b,c</sup> Bao Li <sup>b</sup>

<sup>a</sup>*College of Sciences, China University of Petroleum, Qingdao 266555, China.*

<sup>b</sup>*State Key Laboratory of Information Security (Graduate University of Chinese Academy of Sciences), Beijing 100049, China.*

<sup>c</sup>*Department of Mathematics, Putian University, Putian, Fujian 351100, China*

---

## Abstract

A general construction of binary sequences with low autocorrelation are considered in the paper. Based on recent progresses about this topic and this construction, several classes of binary sequences with optimal autocorrelation and other low autocorrelation are presented.

*Key words:* cryptography, sequences, correlation, CDMA

---

## 1 Introduction

$I_{0022}^3$  Pseudo-random sequences with low cross correlation can be employed in CDMA communications to combat interference from the other users who share a common channel and in stream cipher cryptosystems as key stream generators to resist cross-correlation attacks [5,2]. Given two binary sequences  $a = a(t)$  and  $b = b(t)$  of period  $N$ , the periodic correlation between them is defined by

$$R_{a,b}(\tau) = \sum_{t=0}^{N-1} (-1)^{a(t)+b(t+\tau)}, 0 \leq \tau < N,$$

---

\* This work is supported by the National Natural Science Foundations of China (No.61170319), the Natural Science Fund of Shandong Province (No.ZR2010FM017), the Fundamental Research Funds for the Central Universities(No.11CX04056A) and the China Postdoctoral Science Foundation funded project (No.119103S148)

*Email address:* yantoji@163.com (Tongjiang Yan).

where the addition  $t + \tau$  is performed modulo  $N$ . If  $a = b$ ,  $R_{a,b}(\tau)$  is called the (periodic) autocorrelation function of  $a$ , denoted by  $R_a(\tau)$ , or simply  $R(\tau)$  if the context is clear, otherwise,  $R_{a,b}(\tau)$  is called the (periodic) cross-correlation function of  $a$  and  $b$ . Defining the set

$$C_a = \{0 \leq t \leq N - 1 : a(t) = 1\}$$

the support of  $a(t)$ , then

$$R_a(\tau) = N - 4(|C_a| - |(\tau + C_a) \cap C_a|). \quad (1)$$

The optimal values of out-of-phase autocorrelation of binary sequences in terms of the smallest possible values of the autocorrelation are classified into four types as follows: If  $N \equiv 0 \pmod{4}$ ,  $R(\tau) = \{0, -4, 4\}$ ; if  $N \equiv 1 \pmod{4}$ ,  $R(\tau) \in \{1, -3\}$ ; if  $N \equiv 2 \pmod{4}$ ,  $R(\tau) \in \{2, -2\}$ ; if  $N \equiv 3 \pmod{4}$ ,  $R(\tau) = -1$ . In the last case,  $R(\tau)$  is often called ideal autocorrelation. For more details about optimal autocorrelation, the reader is referred to [1,4].

In 1995, G. Gong found that most of the known sequences with ideal autocorrelation possess the following interleaved construction [3].

**Definition 1** Fix two positive integers  $T$  and  $K$  where  $T \geq 2$  and  $K \geq 1$ . Given a binary sequence  $a = (a(0), a(1), \dots, a(K-1))$  of period  $K$ . If the binary sequence  $u = (u(0), u(1), \dots, u(KT-1))$  can be given by an  $K \times T$  matrix  $A(u)$  as follows:

$$u = \begin{pmatrix} u(0) & \dots & u(T-1) \\ u(T) & \dots & u(2T-1) \\ \vdots & & \vdots \\ u((K-1)T) & \dots & u(KT-1) \end{pmatrix} \quad (2)$$

which satisfies that each column of  $A(u)$  is a shift of  $a$  or a all zero sequence, then  $u$  is called an interleaved sequence.

Let  $A_i$  be the  $i$ th column. Then  $u = (A_0, \dots, A_{T-1})$ . With the development of interleaved technology, the above definition was generalized to the case that not all nonzero column vector  $A_j$  are required to be shift equivalent. For example, in [8], the case that  $A_j$ 's are equivalent to their complements can be permitted. For more details about the interleaved construction, the reader is referred to [4]. In the paper, we use the generalized definition of interleaved sequences. For the original interleaved sequences, we call them classical interleaved sequences.

Assume the binary sequence  $s(t) = I(a_0(k), a_1(k), a_2(k), \dots, a_{T-1}(k))$  possess a  $(K, T)$  interleaved construction, where each  $a_i(k)$  is a binary column sequence of period  $K$ , and  $L^\tau(s(t))$  denote the left  $\tau$ -shift of  $s(t)$  [6]. If  $\tau = \tau_1 T + \tau_2$ , where  $0 \leq \tau_2 \leq T - 1$ , then

**Lemma 1** [3] *The array form of  $L^\tau(s(t))$  is given by*

$$I(a_{\tau_2}(k + \tau_1), \dots, a_{T-1}(k + \tau_1), a_0(k + \tau_1 + 1), \dots, a_{\tau_2-1}(k + \tau_1 + 1)). \quad (3)$$

In 2001, K. T. Arasu, C. Ding, T. Helleseeth, P. Kumar and H. Martinsen gave a construction of binary sequences with optimal autocorrelation of period  $4N$  by sequences of period  $N \equiv 3 \pmod{4}$  with ideal autocorrelation [1]. Then this construction was generalized in [9] and found to possess interleaved construction [8]. In 2010, X. Tang and G. Gong gave three new interleaved constructions of binary sequences with optimal autocorrelation values [6]. This paper will search more general constructions which can include them and some other new binary sequences with low autocorrelation.

## 2 An Interleaved Sequence and Its Modification

Define a pair of binary sequences  $s$  and  $s'$  by

- Construction A:  $s = I(0_K, a_1, a_2, \dots, a_{T-1})$ ,
- Construction B:  $s' = I(1_K, a_1, a_2, \dots, a_{T-1})$ ,

where  $0_K$  and  $1_K$  are all zero sequence and all one sequence of period  $K$  respectively,  $a_i$ 's are binary sequences of period  $K$ . The balance difference of  $a_i$  is given as  $d(a_i) = 2 \mid C_{a_i} \mid - K$ .

In [6], generalized GMW sequences and their modifications of period  $2^{2n} - 1$  are defined respectively as the above sequences  $s$  and  $s'$  with an additional condition that all  $a_i$ 's are some shifts of ideal autocorrelation sequence  $a$ . Then  $d(a_i)$  is constant and takes value 1 or  $-1$ . If  $d(a_i) = -1$ , we can get a pair of modified sequences  $\bar{s}$  and  $\bar{s}'$  by replacing each  $a_i$  with its complement sequence, and keep their autocorrelation unchanged [4]. So we may assume that each  $d(a_i)$  always takes the value 1 when  $s$  and  $s'$  are generalized GMW sequences and their modifications respectively.

The sequence  $s$  and its modification  $s'$  have the following properties of correlation.

**Theorem 1** *Let  $\tau = \tau_1 T + \tau_2$ ,  $0 \leq \tau_2 \leq T - 1$ .*

$$R_{s'}(\tau) = \begin{cases} R_s(\tau) & \text{if } \tau_2 = 0, \\ R_s(\tau) + 2d(a_{\tau_2}) + 2d(a_{T-\tau_2}) & \text{if } \tau_2 \neq 0. \end{cases}$$

The cross-correlation of  $s$  and  $s'$  is given by

$$R_{ss'}(\tau) = \begin{cases} TK - 2K & \text{if } \tau = 0, \\ R_s(\tau) - 2K & \text{if } \tau_2 = 0, \tau \neq 0, \\ R_s(\tau) + 2d(a_{T-\tau_2}) & \text{otherwise ;} \end{cases}$$

$$R_{s's}(\tau) = \begin{cases} KT - 2K & \text{if } \tau = 0, \\ R_s(\tau) - 2K & \text{if } \tau_2 = 0, \tau \neq 0, \\ R_s(\tau) + 2d(a_{\tau_2}) & \text{otherwise .} \end{cases}$$

**Proof.** To calculate  $R_s(\tau)$ , we need compare sequences  $s = I(0_K, a_1, a_2, \dots, a_{T-1})$  and its  $\tau$ - shift  $L^\tau(s)$ .

If  $\tau_2 = 0$ , from Lemma 1,

$$L^\tau(s) = I(0_K, L^{\tau_1}(a_1), \dots, L^{\tau_1}(a_2), \dots, L^{\tau_1}(a_{T-1})),$$

then

$$R_s(\tau) = K + \sum_{i=1}^{T-1} R_{a_i}(\tau_1). \quad (4)$$

Similarly, we have  $R_{s'}(\tau) = K + \sum_{i=1}^{T-1} R_{a_i}(\tau_1)$ . So  $R_s(\tau) = R_{s'}(\tau)$ .

If  $\tau_2 \neq 0$ , from Lemma 1,

$$L^\tau(s) = I(L^{\tau_1}(a_{\tau_2}), \dots, L^{\tau_1}(a_{T-1}), 0_K, \dots, L^{\tau_1+1}(a_{\tau_2-1})).$$

Thus we have

$$R_s(\tau) = \sum_{i=1}^{T-\tau_2-1} R_{a_i a_{i+\tau_2}}(\tau_1) + \sum_{i=T-\tau_2+1}^{T-1} R_{a_i a_{i-(T-\tau_2)}}(\tau_1 + 1) - d(a_{\tau_2}) - d(a_{T-\tau_2}). \quad (5)$$

Similarly

$$R_{s'}(\tau) = \sum_{i=1}^{T-\tau_2-1} R_{a_i a_{i+\tau_2}}(\tau_1) + \sum_{i=T-\tau_2+1}^{T-1} R_{a_i a_{i-(T-\tau_2)}}(\tau_1 + 1) + d(a_{\tau_2}) + d(a_{T-\tau_2}). \quad (6)$$

From the above Equations (5) and (6), we have

$$R_{s'}(\tau) = R_s(\tau) + 2d(a_{\tau_2}) + 2d(a_{T-\tau_2}).$$

To calculate  $R_{ss'}(\tau)$ , we need compare sequences  $s = I(0_K, a_1, a_2, \dots, a_{T-1})$  and  $L^\tau(s')$ , the  $\tau$ -shift of  $s'$ .

If  $\tau = 0$ ,  $s = I(0_K, a_1, a_2, \dots, a_{T-1})$  compares with  $s' = I(1_K, a_1, a_2, \dots, a_{T-1})$ , then

$$R_{ss'}(\tau) = \sum_{k=0}^{K-1} (-1)^{0+1} + \sum_{i=1}^{T-1} R_{a_i}(0) = -K + K(T-1) = KT - 2K.$$

If  $\tau_2 = 0, \tau \neq 0$ ,  $s = I(0_K, a_1, a_2, \dots, a_{T-1})$  compares with  $L^\tau(s')$ , where

$$L^\tau(s') = I(1_K, L^{\tau_1}(a_1), L^{\tau_1}(a_2), \dots, L^{\tau_1}(a_{T-1})),$$

then, from Equation (4),

$$R_{ss'}(\tau) = \sum_{k=0}^{K-1} (-1)^{0+1} + \sum_{i=1}^{T-1} R_{a_i}(\tau_1) = R_s(\tau) - 2K.$$

If  $\tau_2 \neq 0$ , the  $\tau$ -shift of  $s'$

$$L^\tau(s') = I(L^{\tau_1}(a_{\tau_2}), L^{\tau_1}(a_{\tau_2+1}), \dots, L^{\tau_1}(a_{T-1}), 1_K, L^{\tau_1+1}(a_1), \dots, L^{\tau_1+1}(a_{\tau_2-1})).$$

Then, from the comparison of  $s$  and  $L^\tau(s')$  and Equation (5),

$$\begin{aligned} R_{ss'}(\tau) &= \sum_{i=1}^{T-\tau_2-1} R_{a_i a_{i+\tau_2}}(\tau_1) + \sum_{i=T-\tau_2+1}^{T-1} R_{a_i a_{i-(T-\tau_2)}}(\tau_1 + 1) \\ &\quad - d(a_{\tau_2}) + d(a_{T-\tau_2}). \\ &= R_s(\tau) + 2d(a_{T-\tau_2}). \end{aligned} \quad (7)$$

Similarly,  $R_{s's}(\tau)$  can be calculated.  $\square$

If  $s$  in Construction B changes into  $s'$  in Construction A, then  $s'$  possesses the following properties of correlation:

**Theorem 2** *Let  $\tau = \tau_1 T + \tau_2, 0 \leq \tau_2 \leq T - 1$ . The autocorrelation of  $s'$  is given by*

$$R_{s'}(\tau) = \begin{cases} R_s(\tau) & \text{if } \tau_2 = 0, \\ R_s(\tau) - 2d(a_{\tau_2}) - 2d(a_{T-\tau_2}) & \text{if } \tau_2 \neq 0. \end{cases}$$

*The cross-correlation of sequences  $s$  and  $s'$  is given by*

$$R_{ss'}(\tau) = \begin{cases} TK - 2K & \text{if } \tau = 0, \\ R_s(\tau) - 2K & \text{if } \tau_2 = 0, \tau \neq 0, \\ R_s(\tau) - 2d(a_{T-\tau_2}) & \text{otherwise ;} \end{cases}$$

$$R_{s's}(\tau) = \begin{cases} TK - 2K & \text{if } \tau = 0, \\ R_s(\tau) - 2K & \text{if } \tau_2 = 0, \tau \neq 0, \\ R_s(\tau) - 2d(a_{\tau_2}) & \text{otherwise .} \end{cases}$$

As a consequent result of Theorem 1, we have

**Corollary 1** *For the sequences  $s$  and  $s'$ ,*

$$R_{s's}(\tau) = R_{ss'}(\tau) \iff d(a_{T-\tau_2}) = d(a_{\tau_2}).$$

$$R_s(\tau) = R_{s'}(\tau) \iff d(a_{T-\tau_2}) = -d(a_{\tau_2}).$$

On more special conditions, we have

**Corollary 2** *Let  $d(a_{T-\tau_2}) + d(a_{\tau_2}) = d_0$  be a constant.*

(1) *If  $d_0 = 0$ ,  $s'$  possesses ideal autocorrelation if and only if  $s$  has ideal autocorrelation*

(2) *If  $d_0$  is a nonzero constant, then  $s'$  possesses 3-level autocorrelation if and only if  $s$  has ideal autocorrelation.*

**Corollary 3** *Let  $d(a_{T-\tau_2}) = d(a_{\tau_2}) \neq K$  be a constant.  $R_{ss'}(\tau) = R_{s's}(\tau)$  is 3-valued if and only if the sequence  $s$  has ideal autocorrelation.*

**Remark 1** *Theorems 1, 2 and Corollaries 1-3 can induce that some binary sequences with good correlation can be obtained by changing  $s$  into  $s'$  and its inverse process.*

Several known results will be introduced to verify Corollaries 1–3.

Let  $p$  be an odd prime and  $QR_p$  and  $NQR_p$  denote the quadratic residue and nonquadratic residue of  $p$ . A Legendre sequence  $l(t)$  is defined as

$$l(t) = \begin{cases} 0 \text{ or } 1 & \text{if } t = 0, \\ 0 & \text{if } t \in QR_p, \\ 1 & \text{otherwise.} \end{cases}$$

$l(t)$  is called the first type Legendre sequence if  $l(0) = 1$  otherwise the second type Legendre sequence (denoted by  $l'(t)$ ).

**Lemma 2** [6] *Legendre sequences  $l(t)$  and  $l'(t)$  possess the following autocorrelation. If  $p \equiv 3 \pmod{4}$ ,  $l(t)$  and  $l'(t)$  possess ideal autocorrelation, and if  $p \equiv 1 \pmod{4}$ ,*

$$R_l(\tau) = \begin{cases} p & \text{if } \tau = 0, \\ 1 & \text{if } \tau \in QR_p, \\ -3 & \text{if } \tau \in NQR_p. \end{cases} \quad R_{l'}(\tau) = \begin{cases} p & \text{if } \tau = 0, \\ -3 & \text{if } \tau \in QR_p, \\ 1 & \text{if } \tau \in NQR_p, \end{cases}$$

and each type of Legendre sequences satisfies

$$s(t) - s(p-t) = 0 \text{ if } p \equiv 1 \pmod{4}, \quad (8)$$

$$s(t) + s(p-t) = 1 \text{ if } p \equiv 3 \pmod{4}, \quad (9)$$

where  $t = 1, 2, \dots, p-1$ .

In [7], sequences satisfying Equations (8) and (9) are called symmetric and antisymmetric respectively, and some new sequences with these properties are introduced. Obviously, these sequences can confirm the equivalences in Theorem 1 respectively. Combining Equation (9) with (1) of Theorem 2 can explain that these two types both possess ideal autocorrelation when  $p \equiv 3 \pmod{4}$  [6, Property 2]. Combining Equation (8), Lemma 2 with Theorem 2 can explain the cross-correlations  $R_{ll}$  and  $R_{ll'}$  are equal and 2-valued when  $p \equiv 1 \pmod{4}$  [6, Property 3].

For the twin-prime sequence  $t = I(0_p, L^{e_1}(a_1) + b(1), \dots, L^{e_{p+1}}(a_{p+1}) + b(p+1))$ , where  $e_i = i(p+2)^{-1} \pmod{p}$ ,  $p$  and  $p+2$  are two primes,  $b(i) = 1$  if  $i \in QR_{p+2}$

otherwise  $b(i) = 0$ , and  $a_i = l'$  if  $i \in QR_{p+2}$  otherwise  $a_i = l, i = 1, 2, \dots, p+1$ . If  $p \equiv 1 \pmod{4}$ , then  $p+2 \equiv 3 \pmod{4}$ , by Equation (9),  $b(i) + b(p+2-i) = 1$ , thus  $b(i) = 1$  if and only if  $a_i = l'$  if and only if  $a_{p+2-i} = l$ , and

$$d(L^{e_i}(a_i) + b(i)) = d(L^{e_{p+2-i}}(a_{p+2-i}) + b(p+2-i)) = 1. \quad (10)$$

If  $p \equiv 3 \pmod{4}$ , then  $p+2 \equiv 1 \pmod{4}$ , and by Equation (8),  $b(i) = b(p+2-i) = 1$  if and only if  $a_i = a_{p+2-i} = l'$ . Thus Equation (10) is also right.

The above Equation (10) and Theorem 3 can explain the modified type  $t' = I(1_p, L^{e_1}(a_1) + b(1), \dots, L^{e_{p+1}}(a_{p+1}) + b(p+1))$  possesses 3-level autocorrelation and the equal 3-level cross-correlations  $R_{t't}$  and  $R_{tt'}$ , which are the results of Property 5 in [6].

It is well known that any binary sequence with ideal autocorrelation possesses balanced property, from Theorem 3, if  $s$  is an classical interleaved sequence in construction A [3], then  $s'$  possesses 3-level autocorrelation. Property 1 in [6] can be induced by this result. Moreover, autocorrelation functions of all three generalized sequences  $s$ 's in [6] can be obtained by the above Theorem 1

### 3 Construction of New Sequences with Optimal Autocorrelation

In [6], a new interleaved sequence was defined as

$$u = I(s', L^{\frac{1}{4}+\eta}(s') + 1, L^{\frac{1}{2}}(s) + 1, L^{\frac{3}{4}+\eta}(s) + 1),$$

where  $s$  and  $s'$  are interleaved binary sequences in Constructions A and B respectively. Since the construction of  $u$  is determined by the sequence  $s$ , this section considers the relationship between their autocorrelation functions.

**Theorem 3** *Let  $\mu = 4\mu_1 + \mu_2, \mu_2 = 0, 1, 2, 3$ .*

(1) *If  $d(a_x) = c_1, x = 0, 1, \dots, T-1$ , then the autocorrelation function of the sequence  $u$  is given by*



$$R_u(\mu) = \begin{cases} 4KT & \text{if } \mu = 0, \\ 4R_s(\mu_1) & \text{if } \mu_2 = 0, \tau_2 = 0, \mu \neq 0, \\ 4R_s(\mu_1) + 8c_1 & \text{if } \mu_2 = 0, \tau_2 \neq 0, \\ 0 & \text{if } \mu_2 = 1, \tau_1^+ = 0, \\ -4c_1 & \text{if } \mu_2 = 1, \tau_1^+ \neq 0, \\ 0 & \text{if } \mu_2 = 2, \\ 0 & \text{if } \mu_2 = 3, \tau_2^- = 0, \\ -4c_1 & \text{if } \mu_2 = 3, \tau_2^- \neq 0. \end{cases}$$

(2) If  $d(a_x) + d(a_{T-x}) = 0, x = 1, \dots, T-1$ , then the autocorrelation function of the sequence  $u$  is given by

$$R_u(\mu) = \begin{cases} 4KT & \text{if } \mu = 0, \\ 4R_s(\mu_1) & \text{if } \mu_2 = 0, \mu \neq 0. \\ 0 & \text{if } \mu_2 = 1, \tau_1^- = 0, \\ 4d(a_{\tau_2^-}) & \text{if } \mu_2 = 1, \tau_1^- \neq 0, \\ 0 & \text{if } \mu_2 = 2, \\ 0 & \text{if } \mu_2 = 3, \tau_2^+ = 0, \\ -4d(a_{\tau_2^-}) & \text{if } \mu_2 = 3, \tau_2^+ \neq 0. \end{cases}$$

**Proof.** By Lemma 1 and due to four different values of  $\mu_2$ , the autocorrelation of the sequence  $u$  can be given by the following:

Case 1: If  $\mu_2 = 0$ , then  $R_u(\mu) = 2R_{s'}(\mu_1) + 2R_s(\mu_1)$ .

Let  $\mu_1 = \tau_1 T + \tau_2, 0 \leq \tau_2 \leq T-1$ . Then, by Theorems 1 and 2, we have

(1) if  $\tau_2 = 0$ ,  $R_u(\mu) = 4R_s(\mu_1)$ , (2) if  $\tau_2 \neq 0$ ,  $R_u(\mu) = 4R_s(\mu_1) + 4d(a_{\tau_2}) + 4d(a_{T-\tau_2})$ .

Case 2: If  $\mu_2 = 1$ ,  $R_u(\mu) = R_s(\frac{1}{4} + \eta + \mu_1) - R_{s'}(\frac{1}{4} + \eta + \mu_1) + R_{s's}(\frac{1}{4} - \eta + \mu_1) - R_{ss'}(\frac{1}{4} - \eta + \mu_1)$ .

Let  $\frac{1}{4} + \eta + \mu_1 \equiv \tau_1^+ \pmod T$ ,  $\frac{1}{4} - \eta + \mu_1 \equiv \tau_1^- \pmod T$ , where  $0 \leq \tau_1^+, \tau_1^- \leq T-1$ . Then, by Theorems 1 and 2, we have

$$R_u(\mu) = \begin{cases} 0 & \text{if } \tau_1^+ = \tau_1^- = 0, \\ 2d(a_{\tau_1^-}) - 2d(a_{T-\tau_1^-}) & \text{if } \tau_1^+ = 0 \text{ and } \tau_1^- \neq 0, \\ -2d(a_{\tau_1^+}) - 2d(a_{T-\tau_1^+}) & \text{if } \tau_1^+ \neq 0 \text{ and } \tau_1^- = 0, \\ 2d(a_{\tau_1^-}) - 2d(a_{T-\tau_1^-}) & \text{if } \tau_1^+ \neq 0 \text{ and } \tau_1^- \neq 0. \\ -2d(a_{\tau_1^+}) - 2d(a_{T-\tau_1^+}) \end{cases}$$

Case 3: If  $\mu_2 = 2$ , then

$$\begin{aligned} R_u(\mu) &= -R_{s's}(\frac{1}{2} + \mu_1) + R_{s's}(\frac{1}{2} + \mu_1) - R_{ss'}(-\frac{1}{2} + \mu_1) + R_{ss'}(-\frac{1}{2} + \mu_1) \\ &= 0. \end{aligned}$$

Case 4: If  $\mu_2 = 3$ , then

$$\begin{aligned} R_u(\mu) &= R_s(\frac{3}{4} - \eta + \mu_1) - R_{s'}(\frac{3}{4} - \eta + \mu_1) \\ &\quad + R_{ss'}(\frac{3}{4} + \eta + \mu_1) - R_{s's}(\frac{3}{4} + \eta + \mu_1), \end{aligned}$$

Let  $\frac{3}{4} + \eta + \mu_1 \equiv \tau_2^+ \pmod T$ ,  $\frac{3}{4} - \eta + \mu_1 \equiv \tau_2^- \pmod T$ , where  $0 \leq \tau_2^+, \tau_2^- \leq T-1$ . By Theorems 1 and 2, we have

$$R_u(\mu) = \begin{cases} 0 & \text{if } \tau_2^+ = 0 \text{ and } \tau_2^- = 0, \\ -2d(a_{\tau_2^-}) - 2d(a_{T-\tau_2^-}) & \text{if } \tau_2^+ = 0 \text{ and } \tau_2^- \neq 0, \\ 2d(a_{T-\tau_2^+}) - 2d(a_{\tau_2^+}) & \text{if } \tau_2^+ \neq 0 \text{ and } \tau_2^- = 0, \\ 2d(a_{T-\tau_2^+}) - 2d(a_{\tau_2^+}) & \text{if } \tau_2^+ \neq 0 \text{ and } \tau_2^- \neq 0. \\ -2d(a_{\tau_2^-}) - 2d(a_{T-\tau_2^-}) \end{cases}$$

Then, by Lemma 1 and Theorem 1, the proof can be completed.  $\square$

As a direct corollary of Theorem 3, we consider the following case.

**Theorem 4** *The sequence  $u$  possesses optimal autocorrelation if and only if it satisfies either of the following conditions:*

*Condition 1: the sequence  $s$  has ideal autocorrelation and  $d(a_x) = 1$ .*

*In this case, the autocorrelation function of the sequence  $u$  is given by*

$$R_u(\mu) = \begin{cases} 4KT & \text{if } \tau = 0, \\ -4 & \text{if } \mu_2 = 0, \tau_2 = 0, \mu \neq 0, \\ 4 & \text{if } \mu_2 = 0, \tau_2 \neq 0, \\ 0 & \text{if } \mu_2 = 1, \mu_1 \equiv -\frac{1}{4} - \eta \pmod{T}, \\ -4 & \text{if } \mu_2 = 1, \mu_1 \not\equiv -\frac{1}{4} - \eta \pmod{T}, \\ 0 & \text{if } \mu_2 = 2, \\ 0 & \text{if } \mu_2 = 3, \mu_1 \equiv -\frac{3}{4} + \eta \pmod{T}, \\ -4 & \text{if } \mu_2 = 3, \mu_1 \not\equiv -\frac{3}{4} + \eta \pmod{T}. \end{cases}$$

*Condition 2:  $s$  has ideal autocorrelation and  $d(a_x) = -d(a_{T-x}) \in \{1, -1\}$ .*

*In this case, the autocorrelation function of the sequence  $u$  is given by*

$$R_u(\mu) = \begin{cases} 4KT & \text{if } \mu = 0, \\ -4 & \text{if } \mu_2 = 0, \mu \neq 0, \\ 0 & \text{if } \mu_2 = 1, \tau_1 \equiv -\frac{1}{4} + \eta \pmod{T}, \\ \pm 4 & \text{if } \mu_2 = 1, \mu_1 \not\equiv -\frac{1}{4} + \eta \pmod{T}, \\ 0 & \text{if } \mu_2 = 2, \\ 0 & \text{if } \mu_2 = 3, \mu_1 \equiv -\frac{3}{4} - \eta \pmod{T}, \\ \mp 4 & \text{if } \mu_2 = 3, \mu_1 \not\equiv -\frac{3}{4} - \eta \pmod{T}. \end{cases}$$

Actually, all three constructions of sequences with optimal autocorrelation in [6] can be included in the above Theorem 4. More specifically, autocorrelation of Constructions A and B in [6] can be explained by the equivalence about Condition 1 of the above Theorem 4, and the equivalence about Condition 2 can explain autocorrelation of main parts of Construction C in [6] directly. Moreover, based on our Theorem 3, many binary sequences with low autocorrelation can be constructed by searching more binary sequences with low autocorrelation in Constructions A and B.

## 4 Acknowledgement

This paper was completed while the first author was a visiting scholar at the Department of ECE of University of Waterloo. We would like to express our gratitude to Professor G. Gong. for the supports.

## References

- [1] K. T. Arasu, C. Ding, T. Helleseeth, P. Kumar, H. Martinsen, Almost difference sets and their sequences with optimal autocorrelation, *IEEE Transactions on Information Theory* 47 (7) (2001) 2934-2943.
- [2] J. L. Brown, Crosscorrelation between linearly and nonlinearly distorted versions of a given signal, *Information Sciences* 12 (2) (1977) 93-103.
- [3] G. Gong, Theory and applications of q-ary interleaved sequences, *IEEE Transactions on Information Theory* 41 (2) (1995) 400-411.
- [4] S. W. Golomb, G. Gong, Signal design for good correlation for wireless communication, cryptography. Cambridge University Press, the United States of America, 2005.
- [5] Y. Nawaz, G. Gong, WG: A family of stream ciphers with designed randomness properties *Information Sciences* 178 (7) (2008) 1903-1916.
- [6] X. Tang, G. Gong, New constructions of binary sequences with optimal autocorrelation value/magnitude, *IEEE Transactions on Information Theory* 56 (3) (2010) 1278-1286.
- [7] T. Xiong, J. I. Hall, Modifications of modified Jacobi Sequences, *IEEE Transactions on Information Theory* 57 (2011) 493-504.
- [8] N. Yu, G. Gong, New binary sequences with optimal autocorrelation magnitude, *IEEE Transactions on Information Theory* 54 (10) (2008) 4771-4779.
- [9] Y. Zhang, J. G. Lei, and S. P. Zhang, A new family of almost difference sets and some necessary conditions, *IEEE Transactions on Information Theory* 52 (2006) 2052-2061.